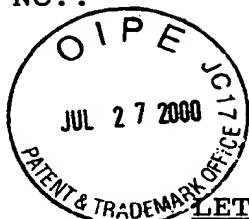


RECEIVED  
500.38618X00  
AUG 21 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE MAIL ROOM

Applicant(s): MAEDA, et al.  
Serial No.: 09/585,358  
Filed: June 2, 2000  
Title: A METHOD FOR MANAGING PUBLIC KEY



LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

July 27, 2000

Sir:

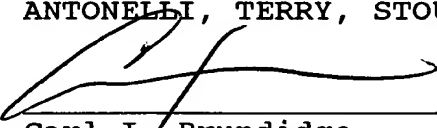
Under the provisions of 35 USC 119 and 37 CFR 1.55, the  
applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 11-155322  
Filed: June 2, 1999

A certified copy of said Japanese Patent Application is  
attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
\_\_\_\_\_  
Carl I. Brundidge  
Registration No. 29,621

CIB/ssr  
Attachment



日本国特許  
PATENT OFFICE  
JAPANESE GOVERNMENT



RECEIVED

AUG 21 2000

TC 2700 MAIL ROOM

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

1999年 6月 2日

出願番号  
Application Number:

平成11年特許願第155322号

出願人  
Applicant(s):

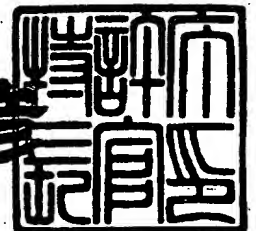
株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 6月29日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



【書類名】 特許願

【整理番号】 KN1057

【提出日】 平成11年 6月 2日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/46

【発明者】

    【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社 日立製作所  
                                 エンタープライズサーバ事業部内

    【氏名】 前田 篤志

【発明者】

    【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社 日立製作所  
                                 エンタープライズサーバ事業部内

    【氏名】 渡部 謙

【特許出願人】

    【識別番号】 000005108

    【氏名又は名称】 株式会社 日立製作所

【代理人】

    【識別番号】 100078134

    【弁理士】

    【氏名又は名称】 武 顕次郎

    【電話番号】 03-3591-8550

【手数料の表示】

    【予納台帳番号】 006770

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵管理方法

【特許請求の範囲】

【請求項 1】 階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられる DNS サーバと、ネットワークに収容されるホストとを備え、前記 DNS サーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理方法において、前記 DNS サーバは、公開鍵を管理する手段と、前記ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納したデータベースとを持ち、第 1 のホストからのドメイン名の情報による第 2 のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第 2 のホストの公開鍵の情報を前記第 1 のホストに応答することを特徴とする公開鍵管理方法。

【請求項 2】 前記 DNS サーバは、第 1 のホストから第 2 のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他の DNS サーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することを特徴とする請求項 1 記載の公開鍵管理方法。

【請求項 3】 前記ホストは、前記 DNS サーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記 DNS サーバに問い合わせることを特徴とする請求項 1 記載の公開鍵管理方法。

【請求項 4】 請求項 1、2 または 3 記載の公開鍵管理方法を実現するための、DNS サーバに設けられる公開鍵を管理する手段の機能を実行するプログラムと、ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納するデータベースと、ホストからドメイン名の情報によって公開鍵の問い合わせを受けたとき該公開鍵管理手段が前記データベースを参照することによりドメイン名に対応する公開鍵をホストに応答する処理を実行するプログラムとを格納したことを特徴とする記憶媒体。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、公開鍵の管理方法に係り、特に、ネットワークにおけるセキュリティ技術に使用される公開鍵暗号システムに使用して好適な公開鍵の管理方法に関する。

## 【0002】

## 【従来の技術】

インターネットを使用してセキュリティ通信を実現する方法として、例えば、IPレイヤのセキュリティプロトコルであるIPSEC(IP SECURITY)が知られており、IPSECに関する技術文献として、例えば、“[RFC1825] Security Architecture for the Internet Protocol. 著者：R. Atkinson 発行：IETF”等が知られている。

## 【0003】

IPSECに付随する鍵管理プロトコルは、公開鍵暗号システムを利用するものであり、鍵管理プロトコルに関する従来技術として、例えば“Simple Key-Management For Internet Protocol. 著者：Ashar Aziz, Tom Markson, Hemma Prafullchandra 発行：IETF”等に記載されたSKIPと呼ばれる技術が知られている。以下、この鍵管理プロトコルについて説明する。

## 【0004】

いま、ネットワーク内にセキュリティ通信を行う2つのホストA、Bがあり、これらのホストA、Bは、IPSECに基づいた共通鍵暗号システムによって暗号通信を行うものとし、ホストAは、ホストBの公開鍵を、ホストBは、ホストAの公開鍵を知っているものとする。

## 【0005】

ホストAとBとは、通信を行うに際して、既知のアルゴリズムを用いて、それぞれ自らの秘密鍵と相手の公開鍵とを組み合わせることで共通鍵を暗号化するための鍵K(A)、K(B)を生成する。ここで、例えば、ホストAがホストBにデータを送信するとき、ホストAは、共通鍵Tを生成し、それを用いてデータを暗号化し、

鍵K(A)を用いて共通鍵Tを暗号化する。ホストAは、暗号化された共通鍵Tの  
情報を含む新たなヘッダをIPヘッダの後に挿入する。受信側のホストBは、自  
らが持つ秘密鍵によって、パケットの中にある暗号化された共通鍵Tを解読し、  
解読した共通鍵Tによって暗号化されたパケットのデータを解読する。そして、  
このようなホストA、B間のセキュリティ通信において、データを暗号化するた  
めの共通鍵は、定期的に更新される。

## 【0006】

前述したようなIPSECに付随する従来技術による鍵管理プロトコルは、セ  
キュリティ通信を行う2つのホストが通信開始前に互いに相手の公開鍵を知っ  
ていることが前提とされている。

## 【0007】

## 【発明が解決しようとする課題】

前述した従来技術による方法は、セキュリティ通信を行おうとする2つのホス  
トが、通信開始前にお互いの公開鍵を自動的かつ安全に交換する方法がなく、そ  
の結果、手渡しによる公開鍵の交換等の方法に頼ることになり、公開鍵の管理が  
複雑になっているという問題点を有している。また、この結果、前述の従来技術  
は、ネットワークの規模が大きい場合、ネットワークの管理者に対する負担が大  
きくなるという問題点を生じさせている。

## 【0008】

さらに、前述の従来技術は、ネットワーク上の認証を伴わない公開鍵の配布を  
行った場合、不正なホストがセキュリティ通信の相手になりすますことを防ぐこ  
とができないという問題点をも有している。

## 【0009】

本発明の目的は、前述した従来技術の問題点を解決し、セキュリティ通信を行  
おうとする2つのホストが通信開始前にお互いの公開鍵を自動的かつ安全に交換  
することを可能にした公開鍵の管理方法を提供することにある。

## 【0010】

## 【課題を解決するための手段】

本発明によれば前記目的は、階層構造を持ち、各階層毎にドメイン名を持つネ

ットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるDNSサーバと、ネットワークに収容されるホストとを備え、前記DNSサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理方法において、前記DNSサーバが、公開鍵を管理する手段と、前記ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納したデータベースとを持ち、第1のホストからのドメイン名の情報による第2のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第2のホストの公開鍵の情報を前記第1のホストに応答することにより達成される。

## 【0011】

また、前記目的は、前記DNSサーバが、第1のホストから第2のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のDNSサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することにより達成される。

## 【0012】

さらに、前記目的は、前記ホストが、前記DNSサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記DNSサーバに問い合わせることにより達成される。

## 【0013】

本発明の目的は、前述の手段を持つ構成以外に、さらに、次に示すような手段を備えることによっても達成することができる。

## 【0014】

すなわち、前記目的は、ネットワークの構成に変更が生じた場合、構成の変化に関係する一部のDNSサーバが、ホストの公開鍵とドメイン名のと対応を格納しているデータベースを更新し、前記以外のDNSサーバがデータベースの更新を行わないようにすることにより達成される。

【0015】

また、前記目的は、前記公開鍵管理手段とデータベースとを備えたDNSサーバと、前記公開鍵を問い合わせる手段を備えたホストとに電子署名を処理する手段を設け、公開鍵問い合わせ及び応答のために出力するパケットに電子署名を付け、電子署名の付いた入力パケットについて、その電子署名を確認し、改竄されている入力パケットを廃棄することにより、パケットの内容が改竄されるのを防止するようにすることにより達成される。

【0016】

また、前記目的は、公開鍵問い合わせ及び応答のために上記公開鍵管理手段とデータベースとを備えたDNSサーバと、前記公開鍵を問い合わせる手段を備えたホストとが、入出力するパケットとして、従来のDNSパケットと同じフォーマットのパケットを用いることにより達成される。

【0017】

また、前記目的は、前記DNSサーバに対してホストが送信する公開鍵問い合わせパケットの中にホストが信用するDNSサーバのドメイン名の情報を含め、公開鍵の情報を応答する前に、前記DNSサーバの公開鍵管理手段に、公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに対して電子署名を要求させ、電子署名の要求を受けたDNSサーバの公開鍵管理手段に、公開鍵応答パケットに電子署名を付けさせ、その電子署名により公開鍵応答パケットに含まれる公開鍵の情報が信用できるか否かを前記ホストの電子署名を処理する手段に判定させ、これにより、不正なホストが自分の公開鍵とアドレスとを公開鍵問い合わせパケットの中にある問い合わせドメイン名に対応しているように見せかけることを防止するようにしたことにより達成される。

【0018】

また、前記目的は、電子署名の要求を受けたDNSサーバが公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバと異なるとき該DNSサーバの公開鍵管理手段は、ドメイン名の階層構造に沿って、上位のDNSサーバに公開鍵応答パケットに対する電子署名を要求し、最終的には公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに公開鍵応答パケットに



電子署名を付けさせることにより達成される。

【 0 0 1 9 】

また、前記目的は、前記ホストの公開鍵問い合わせ手段に、問い合わせるドメイン名に従って信用するDNSサーバを選択させ、公開鍵問い合わせパケットの中に該DNSサーバのドメイン名の情報を含め、公開鍵応答パケットに電子署名を付ける処理を行うDNSサーバの数を減らすことにより公開鍵の取得を効率的なものとする事により達成される。

【 0 0 2 0 】

また、前記目的は、電子署名付きの公開鍵の応答を受けたDNSサーバの公開鍵管理手段に、電子署名付きの公開鍵の応答パケットに含まれる公開鍵、電子署名及び電子署名をしたサーバのドメイン名の情報をキャッシングさせ、ネットワーク及びサーバに無駄な負荷がかかることを防止し、公開鍵の取得を効率化するようにしたことにより達成される。

【 0 0 2 1 】

前述において、ネットワークのドメイン名とアドレスとの対応を解決する手段であるDNSは、DNSを実現するための装置であるDNSサーバの機能を拡張し、ドメイン名と公開鍵との対応を解決する手段を提供する。DNSの実現方法は、例えば、“文献：[RFC1035] Domain Names - Implementation and Specifications 著者：P. Mockapetris 発行：IETF”等に説明されている。

【 0 0 2 2 】

本発明により公開鍵を管理する手段と、ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納されたデータベースとを有する機能拡張されたDNSサーバは、ホストからドメイン名の情報によって公開鍵の問い合わせを受けたとき、前記の公開鍵を管理する手段が前記データベースを参照することにより、問い合わせのドメイン名に対応する公開鍵をホストに応答することができる。これにより、本発明は、ネットワーク上の2つのホストがセキュリティ通信を開始するとき、通信相手のホストのドメイン名に対応する公開鍵を自動的に取得させ、ネットワークにおける公開鍵の管理を容易とすることができる。

## 【 0 0 2 3 】

また、本発明は、公開鍵問い合わせパケットの中にホストが信用するDNSサーバの名前を入れさせ、このホストが信用するDNSサーバによって公開鍵応答パケットに電子署名を付けさせているので、公開鍵応答パケットにある公開鍵が信用できるか否かをホストが判定することができ、不正なホストが自分の公開鍵とアドレスが問い合わせのあったドメイン名に対応しているように見せかけることでセキュリティ通信の相手になりすますことを防止することができる。このとき、公開鍵を取得するためにやり取りする全てのパケットに対して、前述した機能拡張したDNSサーバに電子署名を付けさせることにより、パケットの内容の改竄を防止することができる。

## 【 0 0 2 4 】

## 【発明の実施の形態】

以下、本発明による公開鍵の管理方法の実施形態を図面により説明する。

## 【 0 0 2 5 】

図1はDNSサーバを機能拡張したサーバであるKMS(Key Management Server)の構成を示すブロック図、図2は拡張したDNSクライアントの機能を持つホストの構成を示すブロック図、図3は公開鍵とドメイン名との対応を説明するテーブルの構成を示す図、図4はDNSサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャート、図5はDNSサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャート、図6はDNSクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャート、図7は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図、図8はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図、図9はDNSパケットのフォーマットの構成を説明する図、図10はDNSパケットに含まれる資源レコードのフォーマットの構成を説明する図である。図1、図2、図7、図8において、10はKMS、11、21はネットワーク制御部、12、22はIP処理部、13、23はTCP/U

DP処理部、14は拡張DNS処理部、15はドメイン名/IPアドレステーブル、16、25はドメイン名・公開鍵・電子署名テーブル、17、26は初期保持データ、24は拡張DNSクライアント、27はセキュリティ通信処理部、101はネットワーク、141、241はDNSパケット振り分け部、142はDNS処理部、143は公開鍵問い合わせ/応答処理部、144は電子署名処理部、242はドメイン名リゾルバ、243は公開鍵問い合わせ処理部、244は電子署名処理部、71、75はホストA、B、72~74、76はKMSである。

【0026】

まず最初に、本発明が適用されるネットワークシステム全体の構成及び処理の流れについて図7を参照して説明する。

【0027】

図7に示すネットワークシステムは、ネットワークが階層構造を持ち、各階層毎にドメイン名が与えられており、ドメインを持つネットワークの各階層が1つのKMSを持つように構成されている。ここで、ホストA71がホストB75の公開鍵を取得する場合について考える。この場合、ホストA71は、同一のドメインの階層にあるKMS“1”72に対してホストB75の公開鍵を問い合わせる。このとき、単にホストB75の公開鍵のデータを受け取るのみでは不正な他のホストがホストB75に成りすますのを防ぐことができないので、ホストA71は、信用することができるKMSの電子署名も要求する。今の場合、ホストA71が信用するKMSはKMS“00”74であるとする。また、KMS“00”74の公開鍵は、ホストA71のみならず一般に広く知られ、認証されているものとする。

【0028】

KMS“1”72は、ホストA71からのホストB75の公開鍵のデータの要求に対して、ホストB75の公開鍵のデータを持っていない場合、上位のKMS“0”73に問い合わせるが、持っている場合、ホストA71が信用しているKMS“00”74にホストB75の公開鍵のデータに電子署名を付けるように要求する。また、KMS“1”72は、ホストB75の公開鍵のデータを持っていない場合、ホストB75の公開鍵のデータを持っているKMSに行き会うまで再帰的

に上位のKMSに問い合わせを続ける。KMS “1” 72からの問い合わせを受けたホストB 75の公開鍵のデータを持っているKMSは、KMS “00” 74に電子署名を要求する。

【0029】

電子署名を付けるように要求されたKMS “00” 74は、自らの電子署名を付けたホストB 75の公開鍵のデータをKMS “1” 72に返す。KMS “1” 72は、ホストB 75の公開鍵のデータをホストA 71に返す。この場合、ホストA 71は、元々KMS “00” 74の公開鍵を知っているためそれが信用できるデータか否かを判断することができる。

【0030】

前述した一連の処理によりホストA 71は、ホストB 75の公開鍵を安全に取得することができ、これを使用して、ホストB 75との間でセキュリティ通信を行うことができる。

【0031】

次に、図9、図10を参照して、DNSパケットのフォーマットの構成と、DNSパケットに含まれる資源レコードのフォーマットの構成とを説明する。

【0032】

DNSパケットは、図9に示すように、DNSヘッダ91、問い合わせ部92、回答部93、権限付きネームサーバの名前を表す権威部94、複数の資源レコードを含む付加情報部95から成る。また、図10に示すように、DNSパケットに含まれる資源レコードの1つであるTXTレコードは、名前フィールド101、TYPEフィールド102、CLASSフィールド103、この資源レコードが捨てられずにキャッシュされている時間間隔を示すTTLフィールド104、データ長フィールド105、データフィールド106からなる。

【0033】

複数の資源レコードとしては、TYPEにより識別される複数のものがあり、本発明の実施形態は、複数あるDNS資源レコードの内TXTレコードと呼ばれるTYPE=16の資源レコードに、公開鍵問い合わせ情報及び公開鍵応答情報を入れることとする。また、本発明の実施形態は、公開鍵問い合わせ情報及び公

開鍵応答情報を入れる資源レコードのデータフィールド106の先頭に公開鍵問い合わせ／応答、電子署名要求、または、通常のTXTレコードの区別がつくような識別子1061のフィールドを設けている。

【0034】

なお、TXTレコードについては、前掲のDNSに関する文献の中に説明がある。また、資源レコードとして、前述したTXTレコードの他に、アドレスとドメイン名との対応を示すAレコード（TYPE=1）、メール・エクスチェンジャのドメイン名を示すMXレコード（TYPE=15）等がある。

【0035】

次に、図1を参照して、本発明の実施形態によるサーバであるKMSの構成を説明する。図1において、各ブロックを結ぶ実線はパケットの受け渡しを行う関係を示し、破線はデータの参照を行うことを示す。

【0036】

KMS10は、ネットワーク制御部11と、IP処理部12と、TCP／UDP処理部13と、拡張DNS処理部14と、ドメイン名／IPアドレステーブル15と、ドメイン名・公開鍵・電子署名テーブル16と、初期保持データ17とを備えて構成され、ネットワーク制御部11を介してネットワーク101に接続されている。また、拡張DNS処理部14は、DNSパケット振り分け部141と、DNS処理部142と、公開鍵問い合わせ／応答処理部143と、電子署名処理部144とを備えて構成されている。

【0037】

前述において、ネットワーク制御部11は、KMS10とIPネットワーク101とを接続している。IP処理部12は、ネットワーク制御部11の上位にあって、IP(Internet Protocol)によってやり取りされるパケットの送受信処理を行う。TCP／UDP処理部13は、IP処理部12の上位にあって、TCP／UDP(Transmission Control Protocol／User Datagram Protocol)によってやり取りされるパケットの送受信処理を行う。ここで、特に、TCP／UDP処理部13は、DNSに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張DNS処理部14に送る。逆に、拡張DNS処理部14

は、自ら生成したパケットを送信するとき、その送信すべきパケットをTCP／UDP処理部13に送る。

## 【0038】

拡張DNS処理部14におけるDNSパケット振り分け部141は、TCP／UDP処理部13からDNSパケットを受け取り、図10に示す識別子1061を見てDNS処理部142、公開鍵問い合わせ／応答処理部143、電子署名処理部144の3つの内のどれかにDNSパケットを振り分ける。DNS処理部142は、TCP／UDP処理部13からの従来のDNSパケットを受け取り、ドメイン名とIPアドレスとが対応づけて格納されているデータベースであるドメイン名・IPアドレステーブル15の検索またはエントリの追加を行う。公開鍵問い合わせ／応答処理部143は、他のKMSからの公開鍵の問い合わせを拡張DNSパケットの形でTCP／UDP処理部13から受け取ったとき、問い合わせのあったドメイン名の公開鍵を取得するためにドメイン名と公開鍵とが対応づけて格納されたドメイン名・公開鍵・電子署名テーブル16を検索する。

## 【0039】

ドメイン名・公開鍵・電子署名テーブル16は、図3に示すように、ドメイン名31、公開鍵32、ホストが信用するKMSが付けた電子署名33、電子署名を付けたKMS名34、エントリの生成時点を示すタイムスタンプ35の5つの項目から成る。公開鍵問い合わせ／応答処理部143は、もし、ドメイン名・公開鍵・電子署名テーブル16にエントリがあれば、問い合わせの要求に従って他のKMSへ電子署名の要求を出すか、または、電子署名処理部144によって公開鍵の応答パケットに電子署名を付ける処理を行う。また、公開鍵問い合わせ／応答処理部143は、ドメイン名・公開鍵・電子署名テーブル16にエントリがないとき、他のKMSに対して、問い合わせのあったドメイン名の公開鍵を問い合わせるパケットをTCP／UDP処理部13を通して送信する。電子署名処理部144は、他のKMSからの電子署名要求を拡張DNSパケットの形でTCP／UDP処理部13から受け取ったとき、問い合わせの要求に従って他のKMSへ電子署名の要求を出すか、または、公開鍵応答パケットに電子署名を付ける処理を行う。

【 0 0 4 0 】

また、KMS 1 0 は、初期保持データ 1 7 を持つ。初期保持データ 1 7 は、自分のドメイン名・公開鍵 1 7 1、DNS の親子関係において上位の KMS のドメイン名 1 7 2、DNS の親子関係において下位にあるものの中で信用する KMS のドメイン名・公開鍵 1 7 3 から成る。KMS 1 0 は、他の KMS に公開鍵を問い合わせに行くときにこれらのデータを利用する。

【 0 0 4 1 】

次に、図 2 を参照して本発明により拡張した DNS クライアントの機能を持つホストの構成を説明する。

【 0 0 4 2 】

ホスト 2 0 は、ネットワーク制御部 2 1 と、IP 処理部 2 2 と、TCP / UDP 処理部 2 3 と、拡張 DNS クライアント 2 4 と、ドメイン名・公開鍵・電子署名テーブル 2 5 と、初期保持データ 2 6 と、セキュリティ通信処理部 2 7 とを備えて構成され、ネットワーク制御部 1 1 を介して IP ネットワーク 1 0 1 に接続されている。また、拡張 DNS クライアント 2 4 は、DNS パケット振り分け部 2 4 1 と、ドメイン名リゾルバ 2 4 2 と、公開鍵問い合わせ処理部 2 4 3 と、電子署名確認部 2 4 4 とを備えて構成されている。

【 0 0 4 3 】

前述において、ホスト 2 0 は、KMS と同様に、ネットワーク制御部 2 1、IP 処理部 2 2、TCP / UDP 処理部 2 3 を持ち、IP ネットワーク 2 0 1 に接続されている。TCP / UDP 処理部 2 3 は、DNS に割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張 DNS クライアント 2 4 に送る。逆に、拡張 DNS クライアント 2 4 は、自ら生成したパケットを送信するとき、そのパケットを TCP / UDP 処理部 2 3 に送る。

【 0 0 4 4 】

拡張 DNS クライアント 2 4 内の DNS パケット振り分け部 2 4 1 は、TCP / UDP 処理部 2 3 から DNS パケットを受け取り、DNS ヘッダの中身を見てドメイン名リゾルバ 2 4 2、公開鍵問い合わせ処理部 2 4 3 のいずれかに処理を振り分ける。ドメイン名リゾルバ 2 4 2 は、従来の DNS クライアントと同様に

、ドメイン名に対応するIPアドレスを解決する処理を行う。そして、ドメイン名に対応するIPアドレスを問い合わせる際、ドメイン名リゾルバ242は、TCP/UDP処理部23を通して問い合わせパケットを送信する。ドメイン名リゾルバ242は、問い合わせに対する応答もTCP/UDP処理部23を通して受信する。

## 【0045】

本発明により新たに付加したモジュールである公開鍵問い合わせ処理部243は、ドメイン名に対応する公開鍵を解決する処理を行う。公開鍵問い合わせ処理部243は、新規に得た公開鍵の情報をドメイン名・公開鍵・電子署名テーブル25に保存し、次回に公開鍵を問い合わせに行く前に参照する。電子署名確認部244は、公開鍵問い合わせ処理部243が受け取った公開鍵の情報について、初期保持データ26内の信用するKMSのドメイン名・公開鍵263を参照して、公開鍵の情報に付いている電子署名が信用するKMSのものか否かを判定し、公開鍵の情報が信用できるか否かを確認する。

## 【0046】

公開鍵問い合わせ処理部243は、信用するKMSのドメイン名・公開鍵263が複数ある場合に、公開鍵を問い合わせるドメイン名に応じて信用するKMSのドメイン名・公開鍵263の中から最適な信用するKMSを選択する。ホスト20は、初期保持データ26内に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを持ち、公開鍵問い合わせ処理部243は、公開鍵を問い合わせに行く際に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを参照する。セキュリティ通信処理部27は、公開鍵問い合わせ処理部243が取得した通信相手の公開鍵に基づいて、従来の方法に従ってセキュリティ通信を行う。

## 【0047】

次に、図4に示すフロー、及び、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を示す図8を参照して、本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の図7に示すネットワークにおいて、ホストが通信相手の公開鍵の取得ために行う手順



について説明する。

【0048】

図7において、KMS“0”73、KMS“1”72、KMS“2”76、KMS“00”74は、図1により説明した構成を持つKMSであり、また、ホストA71、B75は、図2により説明した構成の拡張したDNSクライアントの機能を持つホストである。そして、KMS“00”74は、ドメイン名xxを持つネットワーク701に接続され、KMS“0”73は、ドメイン名a.xxを持つネットワーク702に接続されている。また、ホストA71とKMS“1”72とは、ドメイン名b.a.xxを持つネットワーク703に接続され、ホストB75とKMS“2”76とは、ドメイン名c.a.xxを持つネットワーク704に接続されている。

【0049】

ドメイン名は、階層構造を成しており、各KMSは、従来のDNSサーバの役割をも果たしている。また、図8に示す例は、ホストB75の公開鍵の情報をKMS“2”76のみが持っている場合の各KMSの動作を示しており、また、図8に示す各矢印は、ホストA71がホストB75の公開鍵を取得する際に、ホストとKMSとの間やKMSとKMSとの間でやり取りするパケットやパケットに付加する電子署名の形態を示している。パケットの種類は、公開鍵問い合わせ、電子署名要求、公開鍵応答の3通りあり、電子署名の具体的な内容は、図8の枠内の記号を用いて表しているように、次のように定義されているものとする。

【0050】

S(K, [a, b, c]) : 鍵Kによりメッセージ[a, b, c]に電子署名を付与したもの

D(X) : Xのドメイン名

S(X) : Xの公開鍵

T(X) : Xの秘密鍵

IP(X) : XのIPアドレス

KMS(X) : Xが電子署名を要求するKMS

【0051】

以下、ホストA 71が電子署名を要求するKMSがKMS “00” 74であるとして図4に示すフローを説明する。

【0052】

(1) まず、ホストAは、ホストB 75の公開鍵を問い合わせるパケットをKMS “1” 72に送信する。この公開鍵を問い合わせるパケットは、図8に矢印81により示しているように、

S (T (A) , [D (B) , KMS (A) , IP (A) , D (A) ] )

であり、これは、前述の定義から理解できるように、ホストBのドメイン名、ホストAが電子署名を要求するKMS、ホストAのIPアドレス、ホストAのドメイン名よりなるメッセージに、ホストAの秘密鍵により電子署名を行ったものである。KMS “1” 72がホストA 71からホストB 75の公開鍵を問い合わせるパケットを受けたとき、図1に示す電子署名処理部144は、パケットに付いている電子署名を見る。電子署名処理部144は、ドメイン名・公開鍵・電子署名テーブル16からホストA 71の公開鍵を取り出し、パケットの内容が改竄されてないか否かをその公開鍵を使って判定する（ステップ41）。

【0053】

(2) KMS “1” 72は、ステップ41の判定で、問い合わせパケットが改竄されていた場合、そのパケットを廃棄して処理を終了し、問い合わせパケットが改竄されていない場合、図1に示す公開鍵問い合わせ／応答処理部143を動作させ、問い合わせのドメイン名についてドメイン名・公開鍵・電子署名テーブル16にエントリがあるか否か検索する。ここで、タイムスタンプも参照し、一定時間以上過ぎている場合、無効なエントリと見做す（ステップ43、42）。

【0054】

(3) ステップ42の判定で、ドメイン名・公開鍵・電子署名テーブル16にエントリがなかったとき、図7に示すKMS “1” 72の公開鍵問い合わせ／応答処理部143は、問い合わせのあったホストのドメイン名と自分のドメイン名とについてそれぞれが属するネットワークの名前が一致するか否か判定する。例えば、図7において、問い合わせのホストがB 75である場合、B 75の属するネ

ットワークのドメイン名 c. a. x x と KMS “1” 7 2 の属するネットワークのドメイン名 b. a. x x は一致しない（ステップ 4 4）。

【0 0 5 5】

（4）ステップ 4 4 の判定においてネットワークの名前が一致したとき、図 7 の KMS “1” 7 2 は、ホスト A 7 1 に対してホスト B に対する公開鍵が未解決であることを通知する（ステップ 4 5）。

【0 0 5 6】

（5）ステップ 4 4 の判定においてネットワークの名前が一致しなかったとき、KMS “1” 7 2 は、図 1 にける初期保持データ 1 7 内の上位の KMS のドメイン名 1 7 2 を参照して問い合わせ先を調べ、KMS “0” 7 3 にホスト B 7 5 の公開鍵を問い合わせる。この場合の問い合わせパケットは、図 8 に矢印 8 2 により示すように、

S(T(KMS 1), [D(B), KMS(A), IP(KMS 1), D(KMS 1)]) )  
であり、ホスト B 7 5 のドメイン名、ホスト A 7 1 が電子署名を要求する KMS のドメイン名、KMS “1” 7 2 の IP アドレス及び KMS “1” 7 2 のドメイン名をメッセージとし、KMS “1” 7 2 の秘密鍵を電子署名の鍵とする電子署名を付加して構成される。このように、電子署名を付加することによって問い合わせパケットの不正な改竄を防止することができる（ステップ 4 6）。

【0 0 5 7】

（6）次に、KMS “1” 7 2 は、自 KMS に公開鍵を問い合わせた者がホストか KMS かを公開鍵問い合わせパケットの始点 IP アドレスから判定し、公開鍵を問い合わせたのが KMS である場合、処理を終了する（ステップ 4 6 1）。

【0 0 5 8】

（7）ステップ 4 6 1 で、自 KMS に公開鍵を問い合わせた者がホストである場合、公開鍵問い合わせ／応答処理部 1 4 3 は、上位の KMS から公開鍵の応答があるまで一定時間待ち、一定時間内に公開鍵の応答がなく、電子署名付きの公開鍵を取得できなかった場合、処理を終了する（ステップ 4 6 2、4 6 3）。

【0 0 5 9】

（8）公開鍵問い合わせ／応答処理部 1 4 3 は、電子署名付きの公開鍵の応答が

一定時間内にあった場合、その公開鍵を図 1 に示すドメイン名・公開鍵・電子署名テーブル 16 にキャッシングする。このようにキャッシングを行うことにより、別のホストから同じドメイン名について公開鍵の問い合わせがあったときに、公開鍵問い合わせ／応答処理部 143 は、再度別の KMS に公開鍵の問い合わせに行かずに済み、公開鍵を解決する処理を効率的に行うことができる（ステップ 464）。

## 【0060】

(9) 次に、公開鍵問い合わせ／応答処理部 143 は、図 8 の矢印 87 に示すように自らの電子署名をつけた公開鍵応答パケットを公開鍵の問い合わせを受けたホストに返す。この電子署名付きの公開鍵応答パケットは、D(KMS1)、D(B)、S(B)、S(T(KMS00))、[D(B), S(B), D(KMS00)] をメッセージとし、秘密鍵 T(KMS1) を署名の鍵とするものである（ステップ 465）。

## 【0061】

(10) ステップ 42 のデータベースの検索で、問い合わせのドメイン名について、ドメイン名・公開鍵・電子署名テーブル 16 にエントリがあった場合、図 1 に示す公開鍵問い合わせ／応答処理部 143 は、そのエントリに指定された KMS の電子署名が付いているか否かを見る（ステップ 47）。

## 【0062】

(11) ステップ 47 のチェックで、指定された KMS の電子署名がエントリに付いていた場合、公開鍵問い合わせ／応答処理部 143 は、そのエントリにある電子署名付きの公開鍵をホスト A71 に返す（ステップ 48）。

## 【0063】

(12) 一方、ステップ 47 で指定された KMS の電子署名がエントリに付いていなかった場合、公開鍵問い合わせ／応答処理部 143 は、パケットに付いているホスト A71 が信用する KMS と図 1 の初期保持データの上位の KMS のドメイン名 172 を見て、図 7 に示す KMS “0” 73 に電子署名の要求を出す。図 7 に示す KMS “2” 76 がホスト B75 の公開鍵の情報を持っていて、KMS “0” 73 に電子署名の要求を出す場合、図 8 の矢印 84 に示すように、[D(B

）、KMS（A）、IP（KMS 1）、S（B）及びD（KMS 2）] をメッセージとして、KMS “2” 7 6 の秘密鍵を鍵とする電子署名を付けて要求を行う（ステップ 4 9）。

【0 0 6 4】

前述では、図 7 における KMS “1” 7 2 の動作について説明したが、他の KMS “0” 7 3、KMS “2” 7 6 も、前述した KMS “1” 7 2 の場合と同様な動作を行う。

【0 0 6 5】

次に、図 5 に示すフローと図 7 及び図 8 とを参照して、図 1 に示す KMS の各部の動作の中での電子署名の要求と応答とについて説明する。

【0 0 6 6】

（1）いま、図 7 に示す KMS “0” 7 3 が、KMS “1” 7 2 から電子署名の要求を受けたとする。この場合、KMS “0” 7 3 は、図 1 に示ような構成を持つ自装置内の電子署名処理部 1 4 4 を動作させ、パケットに付いている電子署名を見る。電子署名処理部 1 4 4 は、ドメイン名・公開鍵・電子署名テーブル 1 6 から KMS 1 7 2 の公開鍵を取り出し、パケットの内容が改竄されていないか否かを判定する（ステップ 5 1）。

【0 0 6 7】

（2）ステップ 5 1 の判定で、パケットの内容が改竄されていた場合、電子署名処理部 1 4 4 はパケットを廃棄し、KMS “0” 7 3 は処理を終了する（ステップ 5 3）。

【0 0 6 8】

（3）ステップ 5 1 の判定で、パケットの内容が改竄されていなかった場合、電子署名処理部 1 4 4 は、パケットの内容を見て電子署名の要求先が自分自身か否かを判定する（ステップ 5 2）。

【0 0 6 9】

（4）ステップ 5 2 の判定で、電子署名の要求先が自分自身でない場合、電子署名処理部 1 4 4 は、初期保持データの上位の KMS のドメイン名 1 7 2 を参照し、電子署名の要求を上位の KMS に対して出す。図 7 において、ホスト A 7 1 が

電子署名を要求するKMSがKMS“00”74である場合、図8の矢印85に示すように、KMS“0”73からKMS“00”74への電子署名要求パケットは、[D(B)、KMS(A)、IP(KMS1)、S(B)及びD(KMS0)]をメッセージとしKMS“0”73の秘密鍵を鍵とする電子署名を付けたものとなる(ステップ54)。

【0070】

(5) 一方、ステップ52の判定で、電子署名の要求先が自分自身であった場合、電子署名処理部144は、要求されたパケットに対して自分の秘密鍵によって電子署名を付け、要求元のKMSに電子署名付きのパケットを返す。説明している例で、例えば、署名要求に対してKMS“00”74がKMA“1”72へ公開鍵を応答するものとする、その場合の応答パケットは、図8の矢印86に示すように、[D(B)、S(B)及びD(KMS00)]をメッセージとしKMS“00”74の秘密鍵を鍵とする電子署名を付けたものとなる(ステップ55)。

【0071】

次に、図6に示すフローと図7及び図8とを参照して、図2に示す構成のホストの動作を説明する。

【0072】

(1) 図7において、ホストA71がホストB75の公開鍵を取得しようとするものとする。このとき、図2に示す構成を持つホストA71の公開鍵問い合わせ処理部243は、ドメイン名・公開鍵・電子署名テーブル25を検索しホストB75のエントリがあるか否かを調べる(ステップ61)。

【0073】

(2) ステップ61で、ドメイン名・公開鍵・電子署名テーブル25にホストB75のエントリがなかったとき、公開鍵問い合わせ処理部243は、初期保持データ26の信用するKMSのドメイン名・公開鍵263を参照して信用するKMSを選択し、信用するKMSのドメイン名・公開鍵263が複数ある場合、問い合わせるドメイン名より上位にあってそれに最も近いKMSを選択する(ステップ62)。

【0074】

(3) 次に、公開鍵問い合わせ処理部 2 4 3 は、初期保持データ 2 6 内の公開鍵を問い合わせに行く KMS のドメイン名 2 6 2 を参照して、その KMS にホスト B 7 5 の公開鍵を問い合わせる。この場合の公開鍵問い合わせパケットは、図 8 の矢印 8 1 に示すように、[D (B)、KMS (A)、IP (A) 及び D (A)] をメッセージとし、ホスト A の秘密鍵 T (A) を鍵とする電子署名を付加したものとなる (ステップ 6 3)。

【0075】

(4) ホスト A 7 1 は、ステップ 6 3 での問合せに対して、公開鍵応答パケットが返ってきたとき、図 2 の電子署名確認部 2 4 4 を動作させ、公開鍵応答パケットに付いている電子署名が要求した KMS のものであって、かつパケットの内容が改竄されていないかを確認する (ステップ 6 4)。

【0076】

(5) 一定時間以内に公開鍵応答パケットが返ってこないとき、あるいは、ステップ 6 4 で、公開鍵応答パケットに付いている電子署名が要求した KMS のものでないか、パケットの内容が改竄されていると判定された場合、ホスト A 7 1 は、何もせずに処理を終了する。これにより、ネットワーク上にある不正なホストが自らの公開鍵とアドレスが問い合わせのあったドメイン名に対応しているように見せかけることでセキュリティ通信の相手になりすますことを防止することができる。

【0077】

(6) ステップ 6 4 で、公開鍵応答パケットに付いている電子署名が要求した KMS のものであって、かつパケットの内容が改竄されていないと判定された場合、公開鍵問い合わせ処理部 2 4 3 は、その公開鍵応答パケットの内容を見て、ドメイン名・公開鍵・電子署名・署名した KMS のドメイン名の 4 つの組でドメイン名・公開鍵・電子署名テーブル 2 5 にキャッシングする (ステップ 6 5)。

【0078】

(7) ホスト A 7 1 のセキュリティ通信処理部 2 7 は、前述までの処理で取得した公開鍵、あるいは、ステップ 6 1 で見つかった公開鍵を用い、セキュリティ通

信を行うための処理を開始する（ステップ 6 6）。

【 0 0 7 9 】

ホストは、前述した処理を実行することにより、公開鍵を解決する処理を効率化することができる。

【 0 0 8 0 】

前述した本発明の実施形態によれば、ネットワークの 2 つのホストがセキュリティ通信を開始する前に機能拡張した DNS サーバによって通信相手のホストのドメイン名に対応する公開鍵を自動的に取得させることが可能となり、公開鍵の管理の容易化を図ることができる。

【 0 0 8 1 】

また、本発明の実施形態によれば、ホストが指定した DNS サーバによって公開鍵の応答パケットに電子署名を付けさせることができるので、ネットワーク上にある不正なホストが自らの公開鍵とアドレスとが問い合わせのあったドメイン名に対応しているように見せかけることによりセキュリティ通信の相手になりますことを防止することができる。

【 0 0 8 2 】

前述したような本発明は、FD や CD-ROM 等の記憶媒体に本発明を実現するプログラムを格納しておき、このプログラムを DNS サーバ及びホストにインストールして実現することができる。また、本発明は、ネットワークに接続された情報処理装置の記憶媒体に本発明を実現するプログラムを格納しておき、ネットワークを通して DNS サーバ及びホストのハードディスク等の記憶媒体に前述のプログラムをコピーして実現することができる。

【 0 0 8 3 】

【発明の効果】

以上説明したように本発明によれば、ネットワークの 2 つのホストがセキュリティ通信を開始する前に通信相手のホストのドメイン名に対応する公開鍵を安全に自動的に取得することができるため、公開鍵の管理が容易となる。

【 0 0 8 4 】

また、本発明によれば、ネットワーク上にある不正なホストが自らの公開鍵と



アドレスとが問い合わせのあったドメイン名に対応しているように見せかけることによりセキュリティ通信の相手になりすますことを防止することができる。

【図面の簡単な説明】

【図 1】

DNSサーバを機能拡張したサーバであるKMS(Key Management Server)の構成を示すブロック図である。

【図 2】

拡張したDNSクライアントの機能を持つホストの構成を示すブロック図である。

【図 3】

公開鍵とドメイン名との対応を説明するテーブルの構成を示す図である。

【図 4】

DNSサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャートである。

【図 5】

DNSサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャートである。

【図 6】

DNSクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャートである。

【図 7】

本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図である。

【図 8】

ホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図である。

【図 9】

DNSパケットのフォーマットの構成を説明する図である。

【図 1 0】

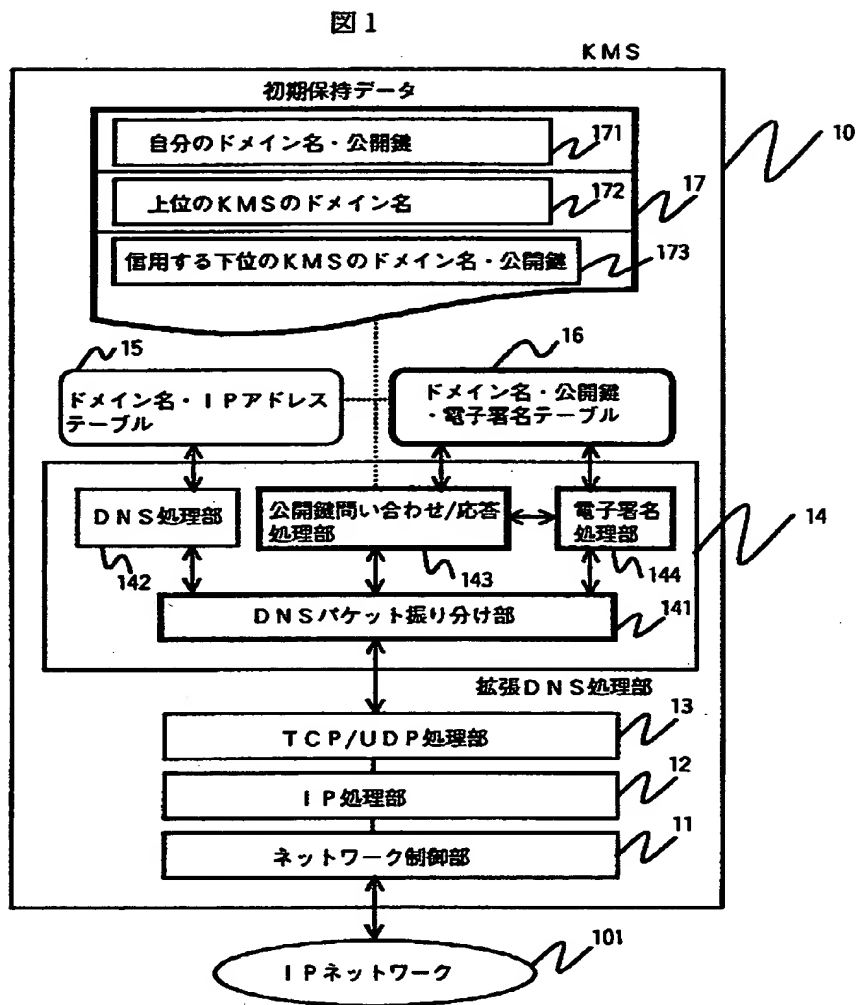
DNS パケットに含まれる資源レコードのフォーマットの構成を説明する図である。

【符号の説明】

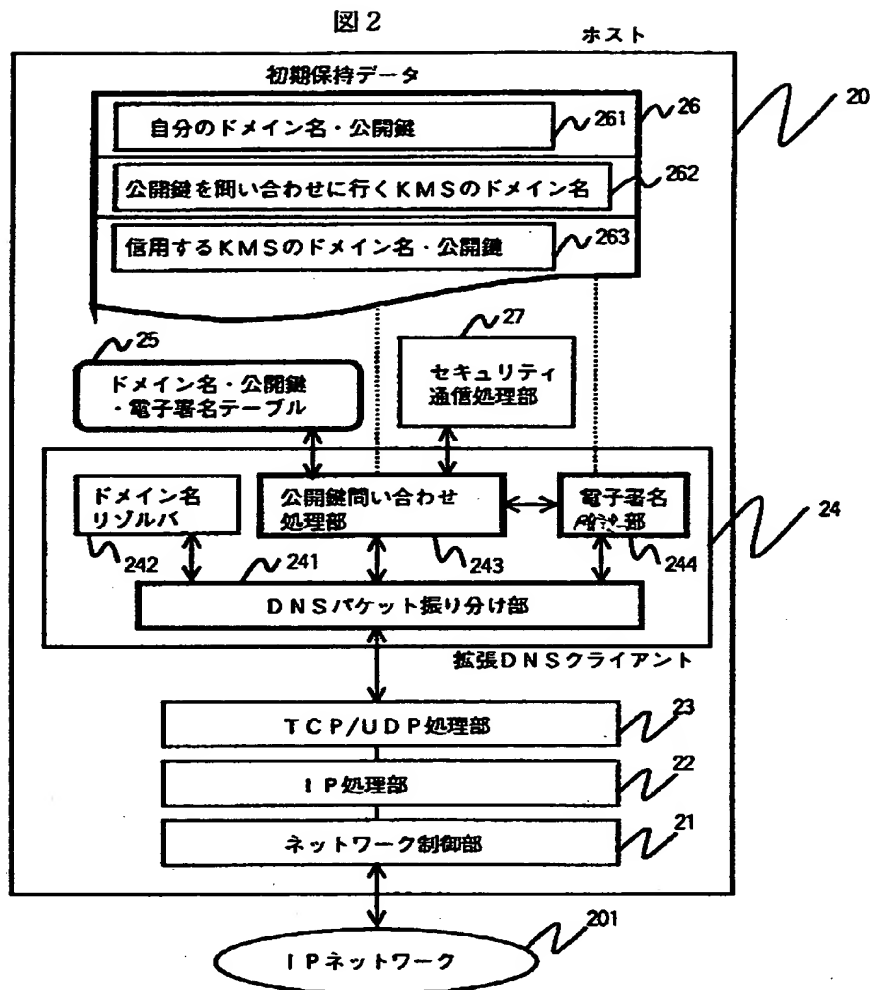
- 1 0    KMS
- 1 1、2 1    ネットワーク制御部
- 1 2、2 2    IP 処理部
- 1 3、2 3    TCP/UDP 処理部
- 1 4    拡張 DNS 処理部
- 1 5    ドメイン名/IP アドレステーブル
- 1 6、2 5    ドメイン名・公開鍵・電子署名テーブル
- 1 7、2 6    初期保持データ
- 2 4    拡張 DNS クライアント
- 2 7    セキュリティ通信処理部
- 1 0 1    ネットワーク
- 1 4 1、2 4 1    DNS パケット振り分け部
- 1 4 2    DNS 処理部
- 1 4 3    公開鍵問い合わせ/応答処理部
- 1 4 4    電子署名処理部
- 2 4 2    ドメイン名リゾルバ
- 2 4 3    公開鍵問い合わせ処理部
- 2 4 4    電子署名確認部
- 7 1、7 5    ホスト A、B
- 7 2～7 4、7 6    KMS

【書類名】 図面

【図 1】



【図 2】



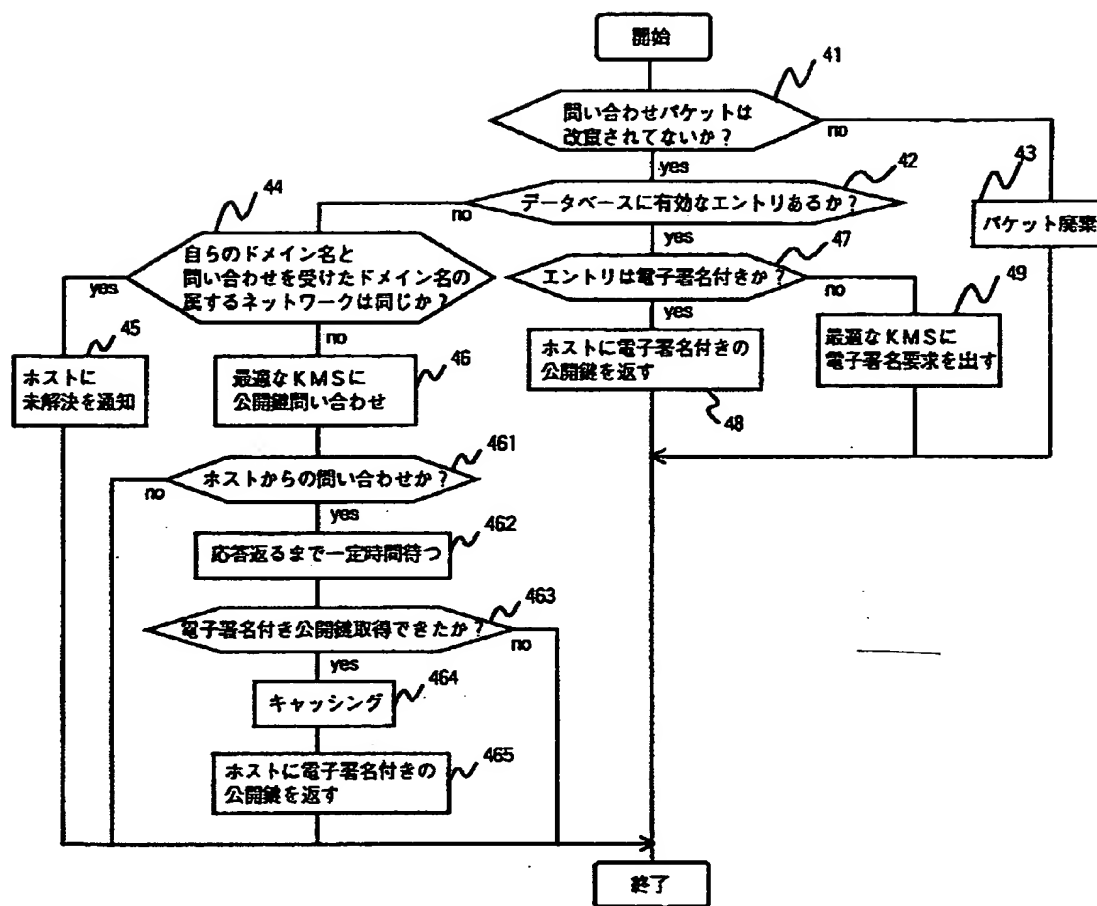
【図 3】

図 3

31 ドメイン名	32 公開鍵	33 電子署名	34 電子署名を付けたKMS名	35 タイムスタンプ

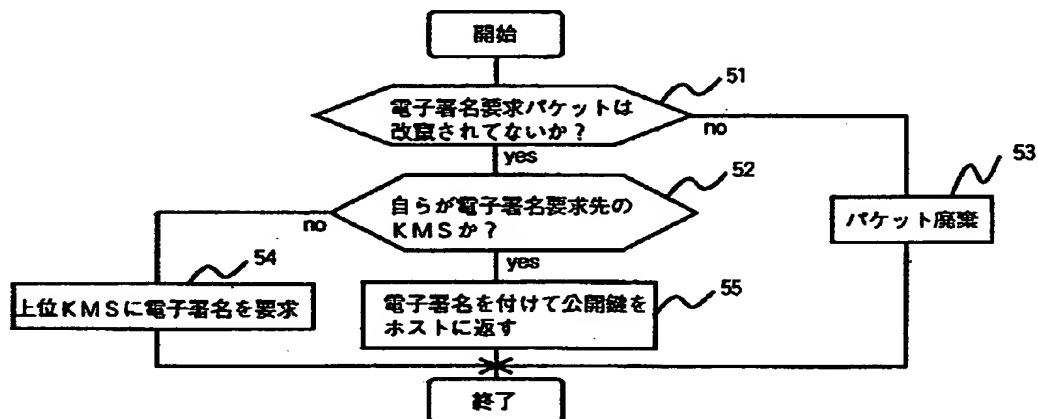
【図 4】

図 4

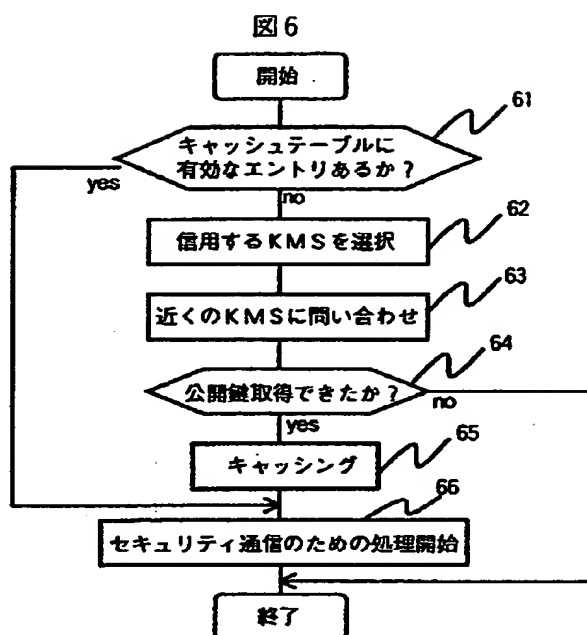


【図 5】

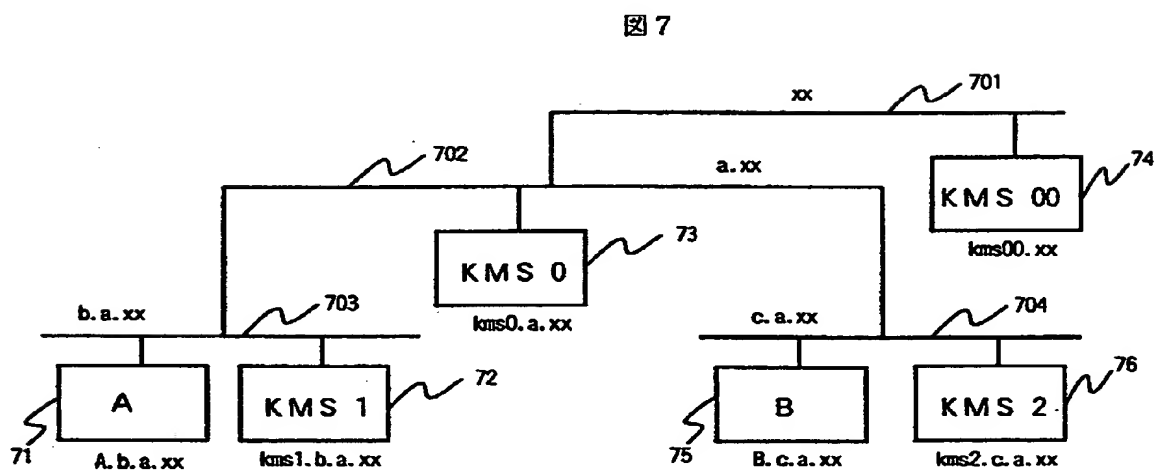
図 5



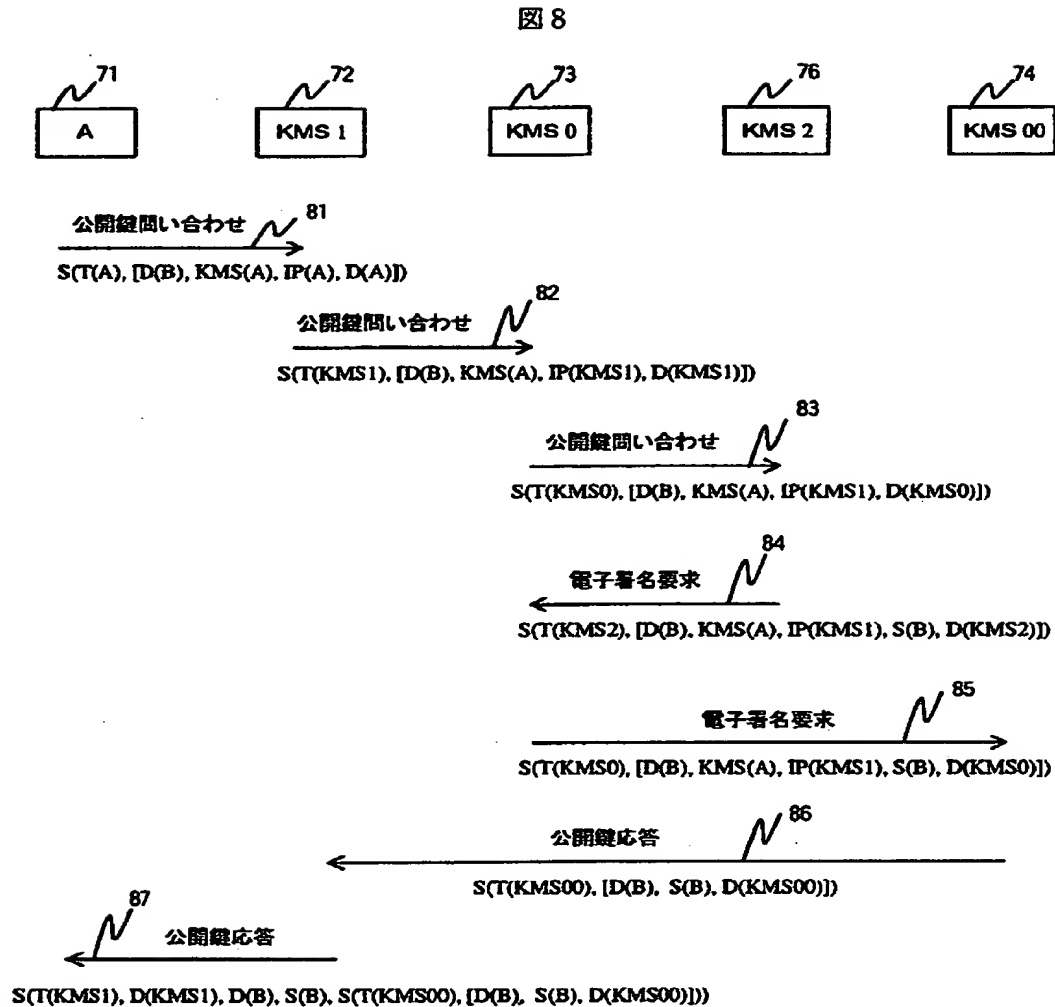
【図 6】



【図 7】



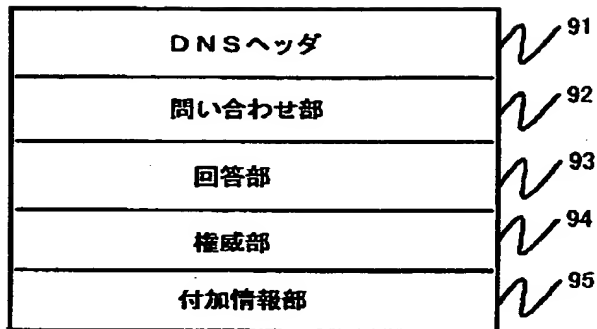
【図 8】



$D(X)$ : Xのドメイン名  
 $S(X)$ : Xの公開鍵  
 $T(X)$ : Xの秘密鍵  
 $IP(X)$ : XのIPアドレス  
 $KMS(X)$ : Xが電子署名を要求するKMS  
 $S(K, [a, b, c])$ : 鍵Kでメッセージ[a, b, c]に電子署名をつけたもの

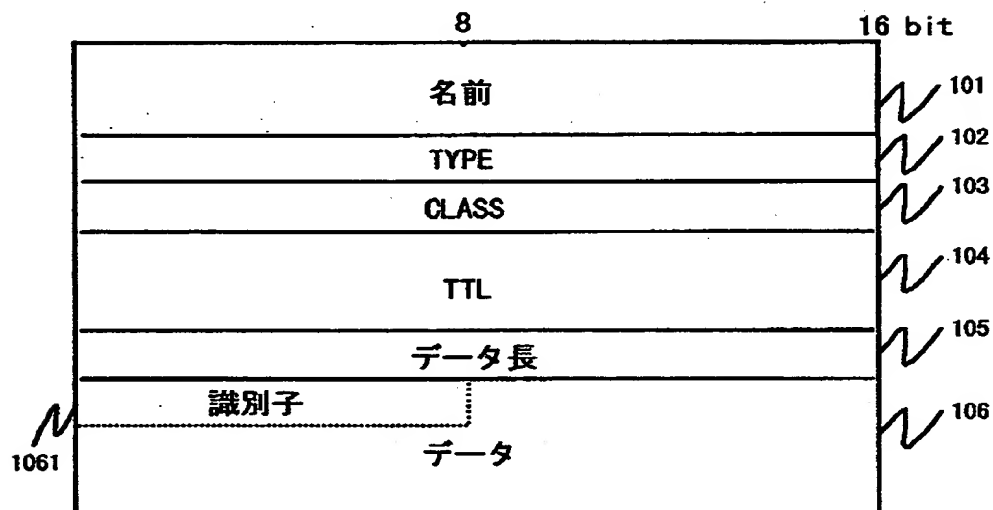
【図 9】

図 9



【図 1 0】

図 1 0





【書類名】 要約書

【要約】

【課題】 セキュリティ通信を行おうとする 2 つのホストが通信開始前にお互いの公開鍵を自動的かつ安全に得ることを可能にした公開鍵管理方法。

【解決手段】 階層構造のドメイン名の構成を持ち、そのドメイン名とアドレスとの対応を管理する DNS サーバが階層毎にあるネットワークにおいて、公開鍵を管理するモジュールとネットワークに属するホストの公開鍵とドメイン名との対応を示すデータベースを各 DNS サーバに設ける。2 つのホストがセキュリティ通信を開始するとき、一方のホストが前述の機能拡張した DNS から通信相手のホストの公開鍵を自動的に取得する。このとき、公開鍵問い合わせパケットの中にホストが信用する DNS サーバの名前を入れさせ、このホストが指定する DNS サーバが、公開鍵応答パケットに電子署名を付ける。ホストは、この電子署名により公開鍵応答パケットにある公開鍵が信用できるかどうかを判定することができ、不正なホストが通信相手になりすますのを防止する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地  
氏 名 株式会社日立製作所